

⑫ 公開特許公報(A)

昭63-191228

⑪ Int. Cl. ⁴	識別記号	庁内整理番号	⑬ 公開	昭和63年(1988)8月8日
G 06 F 9/06	3 3 0	A-7361-5B		
1/00	3 7 0	F-7157-5B		
12/14	3 2 0	F-7737-5B	審査請求	未請求 発明の数 2 (全17頁)

⑭ 発明の名称 コンピュータソフトウェア用の請求システム

⑮ 特 願 昭62-268022

⑯ 出 願 昭62(1987)10月23日

優先権主張 ⑰ 1986年10月24日 ⑱ 米国(US) ⑲ 922689

⑳ 発 明 者	ジョン デイヴィッド グイードマー	アメリカ合衆国 テキサス州 エスト フォレストドライブ 930	77079	ヒューストン ウ
㉑ 出 願 人	ジョン デイヴィッド グイードマー	アメリカ合衆国 テキサス州 エスト フォレストドライブ 930	77079	ヒューストン ウ
㉒ 代 理 人	弁理士 中 村 稔	外 4 名		

明 細 書

1. 発明の名称

コンピュータソフトウェア用の請求システム

2. 特許請求の範囲

(1) デジタルコンピュータのアプリケーションソフトウェアに対しその使用量に基づいてユーザに請求を発する請求システムにおいて、

外部コードを保持するメモリ部分及び請求情報専用のメモリ部分を含んだ取外し可能な請求モジュールと、

コンピュータのためのプログラムを保持した記憶媒体とを具備し、この媒体は、暗号化されない保安プログラムと、暗号化されたアプリケーションプログラムの両方を保持し、保安プログラムは、コンピュータが外部コードを読み取りそしてその外部コードを使用して暗号解読キーを発生し、この暗号解読キーが適当なものである場合にアプリケーションプログラムを使用するように暗号解読するアルゴリズムを駆使する機能と、請求情報

を請求モジュールに入力する機能の両方を行なう機能手段を備えていることを特徴とする請求システム。

(2) コンピュータに保安モジュールが取り付けられ、これに請求モジュールを受け入れて、請求モジュールをコンピュータにインターフェイスするようにした特許請求の範囲第1項に記載の請求システム。

(3) 請求情報専用の請求モジュールのメモリ部分がユーザが追加使用に対して許可を得ていないことを指示する場合には、保安プログラムがアプリケーションプログラムを暗号解読しないようにされた特許請求の範囲第2項に記載の請求システム。

(4) 予め確立された請求許可量が、ユーザに与えられる前に請求モジュールに書き込まれ、保安プログラムは、アプリケーションプログラムの使用中に上記許可量を減少することによって請求情報を入力する特許請求の範囲第3項に記載の請求システム。

(5) 請求情報専用の請求モジュールのメモリ部分のサイズについて予め確立された許可限界は固定され、保安プログラムは、許可されたメモリが完全に占有されるまでアプリケーションプログラムの使用に関する請求情報を上記メモリ部分に書き込む特許請求の範囲第3項に記載の請求システム。

(6) 上記請求モジュールは、EEPROMである特許請求の範囲第1項に記載の請求システム。

(7) 上記EEPROMは、これに指定のラッチコードが与えられるまでここへの書き込み又は読み取りを防止するラッチを有している特許請求の範囲第6項に記載の請求システム。

(8) 上記保安プログラムは、先ず、これが存在する記憶媒体上に請求情報を書き込み、次いで、累積的な請求情報の概要を請求モジュールに周期的に転送する特許請求の範囲第1項に記載の請求システム。

(9) 上記記憶媒体は磁気ディスクである特許請求の範囲第1項に記載の請求システム。

ケーションプログラムの実行を許可すべきであるかどうかを決定する特許請求の範囲第1項に記載の請求システム。

(14) 上記保安プログラムは、請求モジュールから更新チェック情報も読み取り、保安プログラム及びアプリケーションプログラムが適切に更新されたかどうかを決定する特許請求の範囲第1項に記載の請求システム。

(15) 許可されない挿入や妨害を防止するために請求モジュールとコンピュータとの間のデータ転送自体がエンコードされる特許請求の範囲第1項に記載の請求システム。

(16) 常駐リードオンリメモリ及びマイクロプロセッサの両方を含む保安モジュールがコンピュータに取り付けられ、この保安モジュールは、請求モジュールに接続され、コンピュータ及び記憶媒体と請求モジュールとの間の対話及び通信を制御する特許請求の範囲第1項に記載の請求システム。

(17) 上記システムは、相互通信ネットワー

(10) 上記磁気ディスクは、各ディスクに対して独特に埋設されたユーザには分からない特定ディスク識別情報を有し、ディスクの無許可のコピーを、その無許可のコピーを作った元のディスクに対し追跡できるようにした特許請求の範囲第9項に記載の請求システム。

(11) アプリケーションプログラムの暗号化には、上記アルゴリズム及び暗号解読キーによって決定されたようにプログラム内のコードの少なくとも幾つかのコードをエンコードすることが含まれる特許請求の範囲第1項に記載の請求システム。

(12) アプリケーションプログラムの暗号化には、上記アルゴリズム及び暗号解読キーによって決定されたようにプログラム内の命令又はデータをレロケーションすることが含まれる特許請求の範囲第1項に記載の請求システム。

(13) 上記保安プログラムは、請求モジュールから確認番号も読み取りそしてその番号の値を予め決定された予想値に対してテストしてアプリ

クに接続された複数のコンピュータに対して構成され、このネットワークの各コンピュータにおいて単一の請求モジュールが保安モジュールと通信する特許請求の範囲第16項に記載の請求システム。

(18) パーソナルコンピュータのためのアプリケーションソフトウェアプログラムに対しその使用量に基づいてユーザに請求を発する請求システムにおいて、

上記パーソナルコンピュータに取り付けられたハードウェア保安モジュールを具備し、この保安モジュールは、コンピュータが読むことのできる固定の数字内部コードを保持していると共に、請求モジュールインターフェイスも保持しており、

更に、この保安モジュールに物理的に取り付けられてその請求モジュールインターフェイスに電氣的に接続される取外し可能なポータブル式の請求モジュールを具備し、この請求モジュールは、固定メモリと変更可能なメモリとを有し、コンピュータが読むことのできる固定の数字外部コード

はこの固定メモリに記憶されそして請求情報はこの変更可能なメモリに記憶され、そして

更に、保安プログラム及び暗号化されたアプリケーションプログラムを保持したパーソナルコンピュータ用の記憶媒体を具備し、保安プログラムは、パーソナルコンピュータが上記内部コード及び外部コードを読み取って暗号解読キーを発生するようにし、このキーは、所定のアルゴリズムにおいてアプリケーションプログラムをユーザが使用するように暗号解読するのに使用され、保安プログラムは、更に、使用量請求情報を請求モジュールの変更可能なメモリに書き込むことを特徴とする請求システム。

(19) 上記保安プログラムは、アプリケーションプログラムを暗号解読する前に請求モジュールから請求許可情報を読み取り、そして上記保安プログラムは、請求許可が不十分である場合にはアプリケーションプログラムを暗号解読しない特許請求の範囲第18項に記載の請求システム。

(20) 予め確立された請求許可量が請求モジ

要を請求モジュールに周期的に転送する特許請求の範囲第18項に記載の請求システム。

(25) 上記記憶媒体は、磁気ディスクである特許請求の範囲第18項に記載の請求システム。

(26) 保安プログラムによって内部及び外部コードと結合して暗号解読キーを発生しなければならないディスクコードが上記ディスクに保持される特許請求の範囲第25項に記載の請求システム。

(27) 上記磁気ディスクは、各ディスクに対して独特に埋設されたユーザに分からない特定ディスク識別情報を有し、ディスクの無許可のコピーを、その無許可のコピーを作った元のディスクに対して追跡できるようにしている特許請求の範囲第25項に記載の請求システム。

(28) アプリケーションプログラムの暗号化には、上記アルゴリズム及び暗号解読キーによって決定されたようにプログラム内のコードの少なくとも幾つかの文字をエンコードすることが含ま

れるに記憶され、保安モジュールは、使用量に基づいてこの許可量を減少することにより使用請求情報を請求モジュールに書き込む特許請求の範囲第19項に記載の請求システム。

(21) 請求情報に対して別に設定される請求メモリのメモリ量についての予め確立された許可限界が与えられ、保安プログラムは、上記許可限界に達するまで請求情報をそのメモリに書き込む特許請求の範囲第19項に記載の請求システム。

(22) 上記請求モジュールは、EEPROMである特許請求の範囲第19項に記載の請求システム。

(23) 上記EEPROMは、ラッチコードが与えられない限りこのEEPROMへのアクセスを防止する意図されたラッチを有し、保安プログラムは、EEPROMの内容をアクセスするために内部コードからラッチコードを形成する特許請求の範囲第22項に記載の請求システム。

(24) 上記保安プログラムは、請求情報を記憶媒体に頻繁に書き込み、次いで、請求情報の概

れる特許請求の範囲第18項に記載の請求システム。

(29) アプリケーションプログラムの暗号化には、上記アルゴリズム及び暗号解読キーによって決定されたようにプログラム内の命令又はデータをレロケーションすることが含まれる特許請求の範囲第18項に記載の請求システム。

(30) 上記保安プログラムは、請求モジュールから確認番号も読み取りそしてその番号の値を予め決定された予想値に対してテストしてアプリケーションプログラムの実行を許可すべきであるかどうかを決定する特許請求の範囲第18項に記載の請求システム。

(31) 上記保安プログラムは、請求モジュールから更新チェック情報も読み取り、保安プログラム及びアプリケーションプログラムが適切に更新されたかどうかを決定する特許請求の範囲第18項に記載の請求システム。

(32) 許可されない挿入や妨害を防止するために請求モジュールとコンピュータとの間のデー

タ転送自体がエンコードされる特許請求の範囲第18項に記載の請求システム。

(33) 常駐リードオンリメモリ及びマイクロプロセッサの両方を含む保安モジュールがコンピュータに取り付けられ、この保安モジュールは、請求モジュールに接続され、コンピュータ及び記憶媒体と請求モジュールとの間の対話及び通信を制御する特許請求の範囲第18項に記載の請求システム。

(34) 上記システムは、相互通信ネットワークに接続された複数のコンピュータに対して構成され、このネットワークの各コンピュータにおいて単一の請求モジュールが保安モジュールと通信する特許請求の範囲第33項に記載の請求システム。

3. 発明の詳細な説明

産業上の利用分野

本発明は、一般に、コンピュータソフトウェアの市場取引きの分野に係り、特に、最終ユーザに対し一定の購入価格ではなくて使用量に基づく

要したコストを取り戻すために、このような多くのソフトウェア製品の購入価格が、特に、限定配給又は特殊目的のソフトウェアの場合に著しく高いものとなっている。このような高い価格は、或る環境においては、或るソフトウェアを広範囲に販売する上で大きな障害となっており、又、ソフトウェアの出版者が或る市場に製品を浸透させようとする上でも大きな制約となっている。更に、実際にソフトウェアを使ってみなければ、ソフトウェアの適否を判断することが甚だ困難であるから、何人かのユーザは、始めにソフトウェアを作動させずにこのような購入価格を負担することを嫌う。

ソフトウェアの比較的高い購入価格は、多くのソフトウェア出版者に問題として捕らえられている別の現象を招く。パーソナルコンピュータの所有者は、彼が購入したソフトウェアが何等かの形態でコピーに対して防護されていなければ、ソフトウェアの複製コピーをししばしば容易に作るができる。パーソナルコンピュータの何人か

支払構成で市場取引きできるようにパーソナルコンピュータのソフトウェアを機密保持及び/又はエンコード化するシステムに係る。

従来の技術

パーソナルコンピュータの業界は、過去十年にわたって著しく成長を遂げており、パーソナルコンピュータを作動するに適したソフトウェアにおいて大規模な市場を築き上げてきた。多くの会社がコンピュータソフトウェアパッケージを製作して発表するというビジネスをしており、これらのソフトウェアパッケージは、パーソナルコンピュータの所有者が彼らの機械で使用するためにこれらの所有者に市場取引きされる。典型的に、このようなコンピュータソフトウェアパッケージは、一定料金ベースで市場取引きされ、ユーザは、通常、認可書面の協約のもとでソフトウェアのコピーを一定の価格で購入し、ソフトウェアの永続使用権を得ることができる。この業界では、ソフトウェアの発行者がそのソフトウェアの研究及び開発に要した莫大な投下資本や製造及び市場調査に

の所有者がこのようなコピーを作成して彼の友人や知人に配ることがかなり一般的なことになってきている。このように広く頻繁に配られる無断コピーによってソフトウェア製品の市場性が弱くなり、出版者は、妥当な金額が戻るように確保するために製品の各本物コピーに対して更に高い価格を要求することになる。

このようなジレンマに対する1つの解決策は、製造者がコピー防護機構を作り出すことであり、このような機構は、パーソナルコンピュータで無断コピーを行なえないようにする技術的な装置を、パーソナルコンピュータソフトウェアを保持する媒体に含ませた状態で販売できるようにするものである。コピー防護機構は、種々の会社によって種々の技術を用いて実施されている。1つの技術は、プログラムが記憶された磁気ディスクに対し非標準フォーマットを使用することであり、このような非標準的なフォーマットは、そのプログラムが意図されたパーソナルコンピュータのためのオペレーティングシステムではコピーすることが

できない。これまでに使用されている第2の技術は、ディスクをコピーする時にコンピュータが複製できない限定されたフォーマットエラー又は変更された物理的特性をディスクに導入することである。次いで、プログラム中の特殊なコマンドが、ディスクにおいてプログラムを動作させる前にその識別情報をチェックし、これにより、ディスクがコピーでないことを確かめる。最近の傾向として、プログラムを動作させる前にプログラムによってチェックしなければならない物理的な変更をディスクに作るか又はソフトウェアを動作させるためにソフトウェアと共に購入しなければならない「ロック」として知られているハードウェア装置を必要とすることにより物理的な防護機能を果たす第3の種類のソフトウェア防護機構が提案されている。このようなコピー防護機構は、どれも、その多くの防護技術が個々のコンピュータ所有者によって推定されてしまい、コピー防護機構をいかに回避するかが広く伝えられてしまうという点で幾つかの欠点がある。コピーされてしまうであ

る保安モジュールと、コンピュータに含まれた拡張モジュールに設置したりそこから取り外したりできると共に請求情報を書き込んだり読み取ったりするための適当なメモリ位置を含んでいる請求モジュールと、ユーザに付与できるメモリ媒体上の少なくとも2つのプログラムとを具備し、一方のプログラムは保安プログラムでありそして他方のプログラムは暗号化されたアプリケーションプログラムであり、保安プログラムは、保安モジュール及び請求モジュールに質問してそこからのコードを決定し、その情報を使用して暗号解読アルゴリズムを形成すると共に、その暗号解読アルゴリズムを使用してアプリケーションプログラムを暗号解読し、パーソナルコンピュータによって動作できるようにする。

本発明の目的は、プログラムの全体的な保安性又はソフトウェア出版者への適切な戻り収入に危ぐを及ぼすことなくユーザが制限なく何回でもプログラムをコピーできるようにするパーソナルコンピュータ用の機密保持/請求システムを提供

ろう幾つかのディスクのコピー作業を防護できるようにする幾つかのプログラムも市販されている。又、ハードウェアをベースとするシステムは、システムと共に販売されるロックをエミュレートすることのできるハードウェア装置を特別に製作することによって回避することができる。

又、顧客のプログラムを暗号化即ちエンコードし、これを使用するためには、プログラムを暗号解読即ちデコードすることのできる特殊なマイクロプロセッサ又は他の独特なハードウェアを用いなければならないように構成できることも公知技術で一般的に知られている。このようなシステムは、コンピュータに固定布線された特殊な暗号化/暗号解読システムに限定され、従って、システムの方法論がユーザによっていったん推定されてしまうと無断使用を受けがちである。

発明の構成

本発明を要約すると、パーソナルコンピュータのソフトウェアを配給するための請求システムは、ユーザのパーソナルコンピュータに設置でき

ることである。

本発明の更に別の目的は、ユーザが使用量に基づいて支払するというベースでパーソナルコンピュータのソフトウェアにアクセスできるようにし、ソフトウェアパッケージに著しい初期資本をかけることなくソフトウェアを評価し、テストしそして使用することができる一方、ソフトウェアの実際の使用に対してソフトウェア製作者に収入を戻せるようにするソフトウェア普及/請求システムを提供することである。

本発明の更に別の目的は、このような請求システムを逃れることが著しく困難であるように請求システムにおいて配給されるソフトウェアのための保安システムを提供することである。

実施例

本発明の他の目的、特徴及び効果は、添付図面を参照した以下の詳細な説明より明らかとなるう。

ここに開示する本発明のシステムは、ソフトウェアの機密保持及び請求のための最小限の基本

システムであると考えることができ、一連の付加的なオプション又は機能を追加することができる。このシステムにこのようなオプションや機能を追加した場合には、商業的な観点からシステムを益々好ましいものにすることができるか、又はシステムの保安性を促進することができ、このようなオプションや機能は、基本的なシステムに個々に加えてもよいしグループとして加えてもよい。これらのオプションや促進機能の幾つかは、本発明の実際の商業的な実施例に容易に利用される。然し乍ら、本発明の考え方を完全に理解するために、そこに含まれる基本的な考え方の中心が何であるかを先ず理解することが必要である。従って、本発明によって構成された最も簡単なシステムを例示することが必要であろう。

本発明による基本的なコンピュータソフトウェア機密保持/請求システムがパーソナルコンピュータに使用されて第1図のブロック図に示されている。パーソナルコンピュータは、中央処理ユニット(CPU)、常駐メモリ、入力/出力イン

ターフェイス、及び他の関連回路を有するもので、参照番号10で一般的に示されており、他の点では公知の通常のものである。コンピュータCPU及びメモリユニットは、通常、コンピュータソフトウェアプログラムを記憶することのできる1つ以上の媒体、典型的には、第1図に12で一般的に示されたディスク駆動装置を備えている。本発明は、パーソナルコンピュータに現在使用されている一般の磁気ディスク媒体に関連して詳細に説明するが、磁気カートリッジ、光学ディスク、ロムチップ、等のような他の永久メモリ媒体にも等しく適用できることが理解されよう。第1図の実施例において、一般のディスク駆動装置12は、ユーザによって使用されるべきプログラムを含んだ適当にフォーマット化された磁気ディスク14がロードされる。このディスク14は、その物理的な構成については一般のディスクであるが、これに保持されたプログラムは以下で述べるように若干独特なものである。本発明のシステムによって必要とされる独特なハードウェア

は、参照番号16で一般的に示された保安モジュールである。この保安モジュール16は、パーソナルコンピュータ10に電子的に取り付けられる固定布線論理回路である。この保安モジュール16は、いわゆる「オープン」構造のパーソナルコンピュータのシャーシに挿入することのできる拡張カードとして構成することができる。又、保安モジュールは、メインコンピュータのスタンドアロン型の付属品であって、適当な直列又は並列ポートによってコンピュータに取り付けられるものであってもよい。メインコンピュータと保安モジュール16との間の通信方法、即ち、並列であるか直列であるかは、保安モジュール16とパーソナルコンピュータ10との間で転送されるべき情報に対してアドレス路と両方向性データ路とがあるので、あまり重要ではない。

保安モジュール16内には、少なくとも1つの固定のメモリ装置18、好ましくは、PROM、即ち、プログラム可能なリードオンリメモリが配置される。PROM以外の他の固定メモリ装置で

も、ここで必要とされる形式の固定の数字情報を保持できるものであれば、本発明の範囲内で使用することができる。保安モジュールのPROM18は、固定の予め選択された数字コード(ここでは、内部コードと称する)を保持している。この内部コードは、各個々の保安モジュール16ごとに独特なものである。又、保安モジュール16は、その上のどこかに、これも又保安モジュール16に対して独特なシリアル番号を保持することもできる。保安モジュール16のこのシリアル番号(これは、通常は、PROMに保持された内部コードと同じ数値ではない)は、電気的な点からも(PROM又はスイッチの設定のような)且つ又人間が読み取れるという点からも固定のものとされて、保安モジュール16を適当な内部コードと合致できるようにするのが好ましい。

又、保安モジュール16には、これが使用される時に、請求モジュール20も保持される。この請求モジュール20は、保安モジュール16の予め設けられたアクセスインターフェイスに挿入

することのできる取外し可能なメモリ装置である。換言すれば、請求モジュール20は、保安モジュール16に容易に挿入したり取り外したりすることのできる取外し可能なメモリモジュールである。請求モジュール16は、コンピュータ10が保安モジュールを介して読み取ったり書き込んだりすることのできるメモリ部分を有していなければならない。従って、請求モジュールの緻密な媒体は、本発明の範囲内で変更することができる。請求モジュール20としては、磁気、電子、光学又は物理的なデータ記憶技術に基づいて多数の媒体を使用することができる。適当な媒体としては、磁気メモリ部分を有していて保安モジュール16に設けられた読み取り/書き込みインターフェイスに挿入することのできるペーパーカードが含まれる。例えば、保安モジュール16は、パーソナルコンピュータのスタンドアローン型の付属部分であってもよく且つ又請求モジュール20として働く磁気ストリップを保持したペーパーカードが挿入される簡単なカードスロットを有していてもよい。然

モジュール20に予めロードされたデータであってもよいし、情報を書き込むことのできる請求モジュール20上のブランク領域であってもよい。いずれにせよ、本発明にとって重要なことは、請求モジュール20の請求メモリ部分が、コンピュータ10が受け取って処理する情報に基づいてコンピュータ10により変更できるということである。それ故、請求モジュール自体は、外部コードが予め記録された領域と、請求情報がロードされる個別の部分とを有したフロッピーディスクのような取外し可能な磁気記憶媒体として実施することができる。

本発明に用いるためのアプリケーションディスク14は、ユーザが動作しようとする少なくとも1つのコンピュータプログラムを保持している。これは、「アプリケーション」プログラムと称する。本発明によれば、このアプリケーションプログラムは、以下で詳細に述べるように、数値キーによって動かされるアルゴリズムに基づいて暗号化される。それ故、ディスク14は、

し乍ら、本発明の好ましい実施例においては、請求モジュール20がEEPROMで形成される。EEPROMは、電氣的に変更及び消去できるプログラム可能なリードオンリメモリである。このEEPROMの請求モジュール20は、ユーザが容易に取り扱いできるように封入され、そして請求モジュール20を挿入できる保安モジュール16に設けられた簡単な機械的及び電氣的なインターフェイスとインターフェイスするように設計される。

請求モジュール20は、どんな媒体で形成されようと、少なくとも2つのメモリ部分を有している。第1のメモリ部分は、外部コードと称する数値を保持する。請求モジュールの第2のメモリ部分は、請求メモリで構成される。外部コードは、コンピュータにより請求モジュール20から読み取られるように構成された数値である。2つ以上の外部コードが存在し、そして外部コードは2つ以上の部分で構成される。請求メモリは、請求情報を記憶するものであり、この請求情報は、請求

アプリケーションプログラムを暗号化された形態で保持する。又、ディスク14は、暗号化されないスタートプログラムも保持している。更に、ディスク14は、保安プログラムも保持しており、これは、本発明の実施例において所望される冗長保安度のレベルによって暗号化されてもよいしされなくてもよい。保安プログラムが暗号化されない場合には、スタートプログラムは、単に保安プログラムの一部分となる。

第1図に示された基本的なシステムは、その作動中に、次のように動作される。コンピュータ10は通常の状態で作動され、ユーザが動作しようとする暗号化されたアプリケーションプログラムを保持したディスク14がコンピュータのディスク駆動装置12に装填される。通常そうであるように、コンピュータのCPUは、ディスク14の予め指定された部分からプログラムをロードする。ディスク14のその予め指定された部分には、暗号化されていないスタートプログラムが保持され、従って、このプログラムは、

コンピュータ10の常駐メモリにロードされる。次いで、スタートプログラムが動作する。最も基本的な実施例において、スタートプログラムが最初に行なうことは、アクティブな請求モジュールを保持した保安モジュールの存在を確認することである。又、スタートプログラムは、プログラムを進める前にユーザがまだプログラムを動作するための請求クレジットを有していることを請求モジュールから確認する。請求モジュールが存在し且つ請求クレジットがユーザに利用できると仮定すれば、保安プログラムが動作される。保安プログラムは、請求モジュール20から外部コードを読み取る。このコードは、保安プログラムによって利用される予め選択されたアルゴリズムに対して「キー」として働く。全てのアプリケーションプログラムを暗号化したり暗号解読したりするのに単一の特定のアルゴリズムを使用してはならない。実際に、別々のディスク14には別々のアルゴリズムを使用するようにされる。というのは、いかなるディスクの保安プログラムも、

い。又、保安プログラムは、少数の位置を間違えた命令をシフトしてもよい。次いで、保安プログラムは、実行をアプリケーションプログラムに引き継ぎ、ユーザに対して実行を進める。

アプリケーションプログラムを実行するときには、保安プログラムがアプリケーションプログラムの実行を周期的に監視する。これは、プログラムの実行を周期的に保安プログラムに戻すようにして保安プログラムによって呼び出されたルーチンとしてアプリケーションプログラムをフォーマット化することによって行なうこともできるし、或いは又保安プログラムがアプリケーションプログラムの実行に割り込むような1つ以上の割込みによって行なうこともできる。いずれにせよ、この周期的なプロセス中には、保安プログラムがコンピュータ内のアプリケーションプログラムの連続使用を確認し、その使用が続いていると仮定すれば、保安プログラムは、プログラムの使用に基づいて請求データを形成する。この請求データは、非常に頻繁なインターバルでディスク14に

そのディスクのアプリケーションプログラムを暗号化するのに使用されるアルゴリズムに対応するからである。又、使用される各アルゴリズムは、数値キーに基づいたものであって、暗号化するのに用いたものと同じキーを用いてプログラムを暗号解読しなければならないようになっているのが好ましいが、エンコードキーがデコードキーと異なるような2つのキーシステムを使用することもできる。従って、保安プログラムによって使用されるアルゴリズムは、アプリケーションプログラムを暗号化するのに用いたアルゴリズムと反対のものである。保安プログラムは、外部コードからのキーを使用し、暗号解読アルゴリズムを動作させて、暗号化されたアプリケーションプログラムを暗号解読する。保安プログラムは、全アプリケーションプログラムを暗号解読してもよいし、ユーザが一度に使用するアプリケーションプログラムの1つ以上のモジュールのみを暗号解読してもよいし、或いは少数の非常に重要なプログラム命令のアドレス又は位置のみを暗号解読してもよ

記憶され、次いで、請求モジュール20の請求情報領域に周期的に書き込まれる。請求情報を請求モジュール20に入力する方法は、一般に2つある。その1つの方法においては、請求モジュール20の請求メモリに、或る量の予め確立された許可値が与えられ、これは、ユーザに供給される前に請求モジュール20の請求メモリにロードされる。この態様においては、保安プログラムは、アプリケーションプログラムの使用を続けるにつれて請求メモリに含まれた請求クレジット許可値を減少即ち低下させる。ユーザに対してクレジットが延長される第2の方法においては、保安プログラムは、アプリケーションプログラムの実行を継続する時に注目し、ユーザによる使用を指示する情報を請求メモリに書き込む。この方法は、付加的な情報を追加することにより請求メモリを増加させる。請求情報を請求メモリへ搬送するのに減少方式を用いるか増加方式を用いるかに拘りなく、請求は、時間に基づいて行なうこともできるし、或いは、ディスクのアクセス又は異なったモジュ

ールの再ロードといったアプリケーションプログラムによる動作の形式（これは、一般に、ユーザによって使われているアプリケーションプログラムの使用量を減らす）を監視することによって行なうこともできる。

このシステムは、上記した最も簡単な態様においては、アプリケーションプログラムへのユーザのアクセスを、適切に合致された請求モジュール20（これも請求許可を有していなければならない）の存在に基づいて調整する。請求モジュール20は、その外部コードからキーが導出されるアルゴリズムによってディスクットのアプリケーションプログラムがエンコードされるという意味でディスクット14に合致しなければならない。従って、暗号解読数値キーは、ユーザにとって独特のものであるが、暗号化／暗号解読アルゴリズムはディスクットごとに異なってもよい。このシステムは、実施及び保守が最も簡単である。ユーザは、請求モジュール20に設定された限界に達した時に追加の使用許可を得るために請求モジュ

ール20を通常は郵送によってディーラ又は請求センターへ返送することができる。或いは又、請求モジュール20を近代的な中継装置を介して読み取って再ロードすることもできる。従って、ユーザは、ソフトウェアの使用量についてのみ料金が課せられる。更に、コードは周期的に変更できるので、システムの保安性に永久的に背くことは困難である。

この基本的なシステムに追加される付加的な精巧さ及び保安性の第1のレベルは、保安モジュールのPROM18に内部コードを使用することである。この場合は、保安プログラムによってアルゴリズムに使用される暗号解読キーは、単に外部コードから導出されず、内部コードと外部コードの両方から導出されることになる。このように暗号解読キーを導出することは、内部コードと外部コードを単に加えるといった非常に簡単なものであってもよいし、もっと複雑な関係であってもよい。従って、保安プログラムは、どんな方法が選択されていようと、先ず、暗号解読キーを導出

し、次いで、そのキーをアルゴリズムに使用してアプリケーションプログラムを暗号解読する。

システムに対するこのような機能促進の作用は、保安性を追加することである。ユーザは、外部コードを学習するだけではシステムの保安性を免れることができない。内部コードと外部コードを組合せねばならないことにより、ユーザが両方のコードにアクセスできる確率が減少され、システムの保安性を破壊することが非常に困難となる。更に、許可が与えられていないコンピュータへ請求モジュールを移すことが防止される。

このシステムについてのこれらの最も簡単で且つ最も基本的な態様は、ソフトウェアの製作者及び供給者に著しい保安性を与える。外部コード及び内部コードは、個々のユーザにとって独特のものであり、ディスクット14の暗号化されたアプリケーションプログラムは、保安モジュール16と、その特定の個々の保安モジュール16と共に使用する適当な請求モジュール20とを正当に入手した1人のユーザのみによって首尾よく使用

することができる。従って、ディスクット14を使用する場合、ユーザは彼が望むだけ幾つでもコピーをとることができるから、何等かの形式のコピー防護機構を使用する必要はない。然し乍ら、これらコピーの各々は、適当な請求モジュール20を含んだ保安モジュール16と共に使用しない限り、ユーザにとって無効となる。又、暗号化されたアプリケーションプログラムのコピーを余分にとってもユーザはプログラムを動作させることができず、それ故、彼にとって何の利益にもならない。システムの保安性は、これを破壊することが本来的に困難である。というのは、保安モジュールのPROM18の内部コード及び請求モジュール20の外部コードは、予め選択されたもので、各個々のコンピュータにとって独特のものだからである。それ故、この形態で配給されたソフトウェアの1人のユーザが、特定の保安プログラムによって使用されるアルゴリズムと、彼が所有するプログラムの特定の保安モジュール16及び請求モジュール20に使用された内部及び外部コード

とを暴露した場合でも、その情報だけでは、コードが異なるので、別のユーザがシステムの保安性を逃れるには不十分である。更に、暗号化及び暗号解読プロセスに各々別のアルゴリズムを使用する保安プログラムの種々の態様を用いることができる。このように、コピー防護機構を必要とせず、多レベルの保安性が与えられる。

本発明のシステムの保安機能に適合しないことを監視する更に別の方法は、合法的に販売された各々のディスク14を個々に区別することである。即ち、ディスク14には、個々の隠れたシリアル番号を設けることもできるし、又は個々の非機能的なプログラム状の文字シーケンスを設けることもできる。このような方法を採用して保安性が破られた場合には、少なくともその違反を追跡して、保安性のないコピーが作られたディスクをつきとめ、容易に矯正処置をとることができる。

更に、ユーザは、何等かの簡単な形態で使用量に基づいて料金が請求される。減少請求方式を

ラムを家に取り出し、それを所望通りに動作させ、請求モジュールを読み取りのために定期的に供給者に返送することができる。次いで、供給者は、ユーザの使用に基づいてユーザに請求を発することができる。このようなシステムのもとでは、請求モジュールは、典型的に、例えば、1ヵ月といった或る種の一定期間に基づいて供給者によって定期的に交換される。特に、請求モジュールがEEPROMより成るものであって、毎月供給者に容易に郵送することができ且つユーザに返送することができる場合には、ユーザが常に彼のシステムで動作できる請求モジュールを有するように、取引を郵便によって行なうことができる。もう1つの方法は、請求設備によって請求モジュールを離れたところから読み取ることである。モデム及び適当なソフトウェアによりコンピュータ10を離れたところから電話でアクセスして中央の設備で請求モジュール20の請求情報を読み取り、ユーザに料金を課することができる。

以上の説明から明らかなように、本発明は、

用いた場合には、ユーザは、或る使用量についての予めの許可を含む請求モジュール20を彼のソフトウェア供給者から購入することができる。ユーザは、請求モジュール20を家に取り出し、その請求モジュール20に合致するように暗号化されたプログラムディスク14を取り出して、彼が望むようにプログラムを動作させることができる。請求モジュールに含まれた許可の量を越えた場合には、プログラムの実行が停止する。ユーザがそのプログラムをもうそれ以上使用する必要がないと判断した場合には、ユーザがそれを販売者に返却し、彼のディーラへ返送した請求モジュールに含まれている残りの許可量に対するクレジットが与えられる。或いは又、支払能力のある顧客の場合には、その信用度に基づいて請求モジュールを付与することができる。この場合にも、特定の請求モジュール20は、その外部コードに暗号解読キーが合致するアルゴリズムによって暗号化されたアプリケーションプログラムを含むディスク14に合致しなければならない。ユーザは、プログ

特定のアルゴリズムに基づくものではない。実際に、システムは、暗号化に用いられるアルゴリズムの形式にかなりの変化があっても動作することができる。というのは、適切に暗号化されたアルゴリズムがディスクの適当な暗号解読保安プログラムと一緒に使用されると共に、暗号化及び暗号解読が同じ数値キーによって行なわれるからである。ディスクは、暗号化されたアプリケーションプログラムと、これを暗号解読するための保安プログラムの両方を有するようにして供給されるので、コンピュータに実際に物理的に存在する情報、即ち、請求モジュール及び保安モジュールのコード及び請求情報より成る情報は、本質的に、それと共に使用されるプログラムに用いられた暗号化アルゴリズムとは独立したものとなる。

本発明を更に理解するために、アプリケーションアルゴリズムを暗号解読する簡単な方法の例を取り上げることが有用であろう。この簡単な例では、比較的短いコードが使用される。実際には、もっと複雑なアルゴリズム方法論及びもっと長い

コードを用いてシステムの保安性を高めることができる。

上記の説明から明らかなように、本発明の暗号化又は暗号解読手順は、暗号解読キーと称する数値コードによって行なわれる。暗号解読キーは、ランダムに選択され、暗号化されたプログラムを形成するようにアルゴリズムにおいて使用される。それ故、暗号解読手順の最初の段階は、当該プログラムに使用される暗号化キーに対応する適当な暗号解読キーを導出又は形成することである。この暗号解読キーを形成するために、保安プログラムは、保安モジュール 16 の請求モジュール 20 に含まれた外部コードとして知られているコードを読み取る。この外部コードは、保安モジュール 16 に永久的に取り付けられた PROM 18 に含まれた内部コードに加えられる。これら 2 つのコードは、システムによって動作されようとするアプリケーションディスクセット 14 に存在するディスクコードによっても作用される。暗号化キーはランダムに選択されそして保安モジュール 16 に

含まれた内部コードは固定されているので、請求モジュール 20 に含まれた外部コード及びディスクセット 14 に含まれたディスクコードは、これら全てのコードに対するアルゴリズムの作用によって適当な暗号解読キーが形成されるように適切に選択されねばならない。アルゴリズムが簡単な加算で構成されるようなここに示す例においては、これらのコードが通常の 2 進加算によって次のように加えられるだけである。

外部コード	:	1 0 1 0
内部コード	:	1 0 0 1
ディスクコード	:	<u>+ 1 0 1 1 0</u>
暗号解読キー	:	1 0 1 0 0 1

この段階では、暗号解読キーのための数値が形成され、これは、暗号解読アルゴリズムに対しキーとして使用される。明らかなように、コードの長さは用途ごとに異なり、そして種々の 3 つのコード成分のサイズも互いに異なる。

この手順を用いて暗号解読キーが導出されると、次いで、その暗号解読キーを用いてプログラ

ムがセグメントごとに暗号解読される。暗号解読キーは何回も使用され、そのアルゴリズムによって決定された方法でその暗号化されているプログラムコードに適用される。ここでも、説明の目的として、暗号解読のアルゴリズムは、暗号化されたプログラムテキストのビットに暗号解読キーを繰返し論理的に加えるだけであると仮定する。この手順は、次のように処理される。

暗号化されたプログラムテキスト	1011
10 010101	
繰返し暗号解読キー	<u>+1010</u>
01 101001	

暗号解読されたプログラムテキスト [1]0101	
11 111110	

上記の括弧内の数値 [1] は、前方桁上げである。

暗号解読されたプログラムテキストは、プログラムの動作を保安プログラムの適当な段階で移すことのできるコンピュータメモリの部分へロードされる。暗号解読されたアプリケーションプロ

グラムのテキストは、アプリケーションプログラム中にコンピュータによって作用されるべき実際の命令を構成する。上記の簡単な暗号解読手順の場合には、暗号化プログラムが逆の手順となり、暗号化キーが暗号化されていないプログラムテキストから差し引かれて暗号化されたプログラムテキストが形成される。

本発明の手順の 1 つの態様においては、ディスクコードも暗号化することによって付加的な保安性を追加することが所望される。これを行なう場合には、内部及び外部コードからのコードが先ず加えられて、ディスクコード自体を暗号解読する際のキーとして使用されるコードが形成される。次いで、ディスクコードが内部及び外部コードに加えられ、プログラムテキスト自体のための暗号解読キーが形成される。

又、ソフトウェアの動作に対する或る重要な数値、例えば、プログラムのアドレス、又はアドレス自体における幾つかのプログラム命令の位置、或いはフロッピーディスクの或るセクタにおける

情報の相対的な位置を個々に暗号化してもよい。実際に、このようなアドレスが実際のプログラム自体のテキスト内に含まれている場合には、通常プログラムテキスト内でこれらを暗号化しそしてプログラムテキスト全体を暗号化してこれら特定のキーアドレス又は位置の数値を二重に暗号化することもできる。このように二重に暗号化された数値を暗号解読することは単に逆の手順であり、即ち、先ず、プログラムテキスト全体を暗号解読し、次いで、個々の所定のキーアドレス又は位置数値を暗号解読する。

このような一般的な機構内では、暗号解読キーを形成するアルゴリズムとプログラムテキストを暗号解読するアルゴリズムの両方を大きく変えることができる。演算もしくは代数アルゴリズムが好ましいが、簡単さもしくは複雑さの程度を変えるための他のアルゴリズムを用いることもできる。例えば、暗号解読キーを形成する場合には、種々のコードを一括に加えるのではなく、それらを2進形態で順次に配置して、長い数値を形成し、

能させるためにそれらを順序付けし直さねばならないような形態でこれらセグメントをディスク上14上に分布させることもでき、このような再順序付け方法は、当該アルゴリズムによって決定することができる。この場合も、これら全ての態様は、順不同となった命令を暗号解読プログラムによってスクランブル解除し、アプリケーションプログラムを適切に読み取って実行できるように終始一貫した方法で実施しなければならない。

第2図のフローチャートは、本発明によってアプリケーションプログラムを適切に動作させるためにスタートプログラム及び保安プログラムがたどらなければならない一連の段階を一般的に示している。スタートプログラム及び保安プログラムは、保安プログラムが暗号化されていない場合には1つのプログラムと考えることができる。本発明の或る態様においては、保安プログラムを暗号化しそしてこれをスタートプログラムによって暗号解読することが所望される。説明上、保安プログラムは暗号化されておらず、2つのプログラ

これを暗号解読キーとして用いることもできる。プログラムテキストを暗号解読するためのアルゴリズムは、データをビット位置づつ又は所定単位サイズでシフトする動作を含むことができ、これは、標準バイト長さの命令に対応してもよいしなくてもよい。というのは、データをシフトする方法及びタイミングは、このような形態において暗号解読を適宜利用できるように終始一貫したものであるからである。換言すれば、ここで使用する「暗号解読」という語は、文字、用語又は文字シーケンスをエンコードすることのみに限定されるものではなく、暗号化された形態でのプログラムの効果的な動作を阻止し、暗号化/暗号解読キーをベースとしそしてそのキーで容易に暗号解読できるようにするアプリケーションプログラム又はそのコードの再構成も意味するものとする。例えば、種々のコード又はプログラムにまつわる命令シーケンスをレロケーションしたり回転したりすることを必要とする暗号化ルーチンをもたせることもできる。又、プログラムのセグメントを機

能は、第2図に1つのフローチャートとして示されたようなものとなる。このプログラムは、先ず、ディスクからロードされ、参照番号22で示すように始動命令を読み取る段階から始まる。次いで、プログラムは、プログラムステップ番号24で示されたように、一連のアンチ・デモンテストを行なう。デモンとは、コピー防護識別のテストを監視し、次いで、たとえプログラムが非合法的なコピーであったとしても適当な模擬識別応答を発生するようにパーソナルコンピュータにおいて実施されるプログラム又はハードウェアである。デモンは、一般に、RAMメモリに配置されるが、理論的には、内部ROMメモリに常駐されるデモンを形成することが可能である。このプログラムステップ24は、これら装置の存在をテストし、それらを回避するか又はそれらが存在する場合にその動作を回避するように適宜働くものに過ぎない。プログラム動作のステップ番号24は、保安モジュール16に配置されたPROM18から情報を読み取ることである。この情報は、PROM18

に保持された内部コードを含みそして又保安モジュール16に保持された固定布線シリアル番号も含む。PROMから読み取られた情報を用いて、請求モジュール20であるEEPROMへ与えられるべきラッチコードが発生される。EEPROMの請求モジュール20は、これにアクセスするためにこのモジュールに適当なラッチコードを与えねばならないようなラッチ機構を有しているのが好ましく、このステップでは、このコードが形成される。プログラムステップ番号28は、この計算が行なわれることを示すと共に、ラッチコードがEEPROMに送られてEEPROMに対して読み取り及び書き込みを行なえることを示す。EEPROMから読み取りを行なう第1のステップは、ステップ番号30において行なわれ、請求モジュール20自体の中の請求メモリ位置に関して更新チェックが行なわれる。この更新チェック30（システムのオプションである）では、プログラムによって請求モジュール20のメモリ内の所定の位置が検査され、ソフトウェアの現在の更

新状態、即ち、解除状態がチェックされる。アプリケーションプログラム又は保安プログラムは定期的に更新されそして請求モジュール20は定期的に交換されるので、アプリケーションプログラムの更新について請求モジュール20に入れられた情報をこの時点で読み取ることができる。この更新情報は、ユーザに通知するのに使用することもできるし或いは供給者が全てのプログラムコピーを確実に更新したい場合にはそれ以上のシステム動作を防止するように使用することができる。換言すれば、システムプログラムは、保安プログラムのこのバージョンが絶対的であることを請求モジュールの情報が指示する場合に、プログラムの実行を停止する。ステップ番号32において、適当な請求許可情報が請求モジュール20のEEPROMから読み取られ、プログラムは請求情報を評価することができる。判断ステップ番号34においては、請求モジュール20から得た請求許可情報が分析されて、請求モジュールが一杯であるかどうか又はクレジットの限界を越えたかどうか

かが判断される。いずれかの状態が真であって、ユーザがアプリケーションプログラムを利用するに充分な許可値がもはやない場合には、プログラムは、直接ステップ36に進んで停止する。請求モジュールが、アプリケーションプログラムをユーザが使用するための現在クレジット即ち許可値をまだ含んでいる場合には、処理が続行される。

次のステップ40では、保安プログラムがスタートプログラムと別のものである場合に論理的に保安プログラムの一部分である手順が開始されるが、これら2つのプログラム間の境界は、或る程度明確にすることができる。ここでEEPROMの請求モジュール20へのアクセス権を得たプログラムは、EEPROMから、暗号解読アルゴリズムに使用される外部コード（1つ又は複数）を読み取る。次のステップ42においては、プログラムが、内部コード及び外部コードを、ディスク14から読み取ったディスクコードと共に使用して、暗号解読キーを形成する。この暗号解読キーは、前記したように、アプリケーションプ

ログラムのための暗号化／暗号解読アルゴリズムにおいてキーとして用いられる数値である。プログラムは次いでステップ44へと進み、暗号解読及び位置設定アルゴリズムにおいてキーが実行される。このアルゴリズムは、プログラムコードの暗号解読セグメントに作用して、暗号化されたテキストから平易な暗号化されないコンピュータプログラムテキストを形成すると共に、位置設定機構としても用いられて、ディスク14上の種々の位置にスクランブル形態で配置された種々のプログラムセグメントをスクランブル解除することができる。次いで、プログラムは、ステップ44へ進み、種々のプログラムセクタが暗号解読されると共に、それによって得られた暗号解読されたプログラムテキストがアプリケーションプログラムを適切に実行するのに適した順序でRAMにおいて組み立てられる。

又、暗号解読された実際のアプリケーションプログラム内で、暗号化されたアプリケーションプログラムを形成する際に暗号化及び保安プロセ

スの一部分として故意に命令の位置が変更されていることが考えられる。本発明のシステムの構造においてこのオプションを使用する場合には、これらの位置を変えられた命令の配置及びレロケーションが内部コード及び外部コードによって決定され、これらのコードは、この場合にも、位置を変えられたプログラム命令の配置を決定するキーを形成するのに用いられる。本発明においてこのオプションを使用する場合には、このような位置の変わった命令をレロケートすると共に常駐メモリにおいて適当な形態でこれらをレロケートしてアプリケーションプログラムが適切に実行できるようにするためにこの時点でプログラムステップ48が必要となる。又、本発明におけるオプションの追加の保安特徴として、プログラムは、ディスエーブル命令を取り出し、コピー防止命令をオペレーティングシステム又はパーソナルコンピュータに含まれた他の常駐命令に加えて、意図されないやり方でアプリケーションプログラムの動作が止まるのを防止する。それに関連した手順が52

れた計算の回数の測定によって行なうこともできる。周期的なインターバルで、適当な請求目標を通過したと判断した時に、保安プログラムはステップ90に進み、ここでは、アプリケーションプログラムが保持されたディスクセット14にアプリケーションプログラムの使用量情報が書き込まれる。ディスクセット又はハードディスクが使用される場合にはハードディスクに請求情報をこのように書き込むことは、比較的頻繁に、おそらくは、30秒又は1分に1回という割合で行なわねばならない。同時に、その前に書き込まれた数値を読み取ってメモリに存在する記録と比較し、コンピュータがオフにされるか又はシステムの請求情報を変更するような試みがなされた場合に生じるであろう請求シーケンスの変更が起こっていないことを確かめるのが好ましい。より長い時間周期、おそらくは、15分ないし30分の経過時間インターバルにおいて、保安プログラムは、請求情報を請求モジュール20自体に書き込まねばならない(ステップ62)。この情報は、2つの方法で

において実施され、コピー又は割込みコマンドが評価されてそれらが適当であるかどうか判断される。ステップ52が実施される場合には、各コピー又は割込みコマンドが評価され、それが適当であるかどうか論理ステップ54として判断され、そのコマンドが不適当であると判断された場合には、プログラムが56において実行を停止する。

ユーザがシステムを正しく動作させる場合には、アプリケーションプログラムが実行される。アプリケーションプログラムが実行される間には、保安プログラムがプログラム実行の全制御を維持し、その実行を監視することが必要である。この保安プログラムは、ステップ58によって示されたように、アプリケーションプログラムの使用量を測定する。この測定は、アプリケーションプログラムの動作時間を単にカウントするだけで行なうこともできるし、或いは又、アプリケーションプログラムの出版者の請求戦術及びアプリケーションプログラム自体の目的にもよるが、プログラムの動作を介しての或るループの測定又は実行さ

与えられる。請求モジュールが加算情報を受け取った場合には、プログラムは、請求モジュールの請求メモリ部分に肯定データを書き込む。請求モジュールに予めセットされた許可量が与えられている場合には、ステップ62においてその許可量からの減算が行なわれて、ユーザに許された残りのクレジットを表わす新たな残余が生じる。次いで、プログラムは、ユーザが処理を進めるに十分な請求許可量が請求モジュールにまだあることを決定するために請求許可量をテストする。もしなければ、プログラムは直ちに停止する。請求許可量が存在すれば、ユーザによって終わらされるまでプログラムの実行を続けることができる。

使用量に関するデータの転送についての保安性を向上させることが所望される。これが所望される場合には、使用量データがコンピュータのRAMメモリにある時に、使用量データからチェック和が作られ、使用量データとチェック和の両方がエンコードされる。エンコードされた数値は、次いで、ディスクに書き込まれる。ディスクと請

求モジュールとの間のデータ転送は、エンコード動作によって同様に保護することができる。

又、保安プログラムの種々の部分に配置された保安回避機構に対して付加的なアンチ・デモンテスト又は他のテストを行なう、システムの全保安動作の策略が損なわれないようにすることも所望される。

本発明のシステムに含まれるもう1つのオプションは、確認数値を挿入することであり、この数値は、順次の又はエンコードされた数値であって、システムによって請求モジュールからディスクセット14に書き込むことができるものである。次いで、システムは、プログラムにおける種々の時間に請求モジュールに適切な確認数値が存在することを確かめて、システムに無断で割込みが生じたり不適切な使用が生じたりしないように常時チェックを行なう。例えば、各々の請求モジュールは、その次の手前の確認数値から導出することのできる確認数値を含む。このようにして、システムがその同じ又は次の確認数値をテストする場

ジュールのPROMと請求モジュールのEEPROMとの両方に直結させることができる。保安モジュールマイクロプロセッサは、請求モジュールと主マイクロプロセッサ又はディスクとの間のデータ転送を暗号化したり暗号解読したりすることができる。保安モジュールマイクロプロセッサは、保安モジュール又は請求モジュールのPROMに保持された独特なルーチンによって暗号解読キーを発生する。プログラムの使用量又は請求情報は、保安モジュールマイクロプロセッサへ直接転送され、請求モジュールへ周期的に転送するためにそこに累積される。

このマイクロプロセッサを装備した保安モジュールは、この保安モジュールで2つ以上のパーソナルコンピュータに対応できるという点で機能が向上される。多数のパーソナルコンピュータがローカルエリアネットワークに接続された会社のような大規模の構成については、請求集中装置と称される単一のプロセッサがネットワーク上のコンピュータの請求モジュールをポーリングし、シ

合には、許可されない請求モジュールの使用が防止されるが、この保安レベルは冗長であるといなすことができる。或いは又、請求モジュールを周期的に変えるためにプログラム使用量の測定値から確認数値を発生することができる。確認数値を機能させるための最も好ましい方法は、確認数値を暗号化された形態で請求モジュールからアプリケーションプログラムを含むディスクへ転送することである。請求モジュールを変えた時には、確認キーが新たな請求モジュールから読み取られ、前の請求モジュールからの暗号化された確認数値を暗号解読するのに使用される。この暗号解読された確認数値は、アプリケーションプログラムの実行を進める前にその予想値と比較される。更に冗長な保安性をシステムに追加するために本発明の範囲内で他の同様の変更及び修正を行なうことができる。

例えば、本発明の別のより精巧な態様においては、保安モジュール自体に保安モジュールマイクロプロセッサを設けてこのプロセッサを保安モ

システムの各ノードから請求情報を読み取ることが考えられる。請求集中装置は、おそらくはモデムによって請求情報を中央の請求許可装置と通信する。このオプションを実施するために、請求集中装置と通信することのできるマイクロプロセッサが保安モジュールに必要とされる。

本発明は、図示して説明した各部の特定の構成及び配置に限定されるものではなく、本発明の範囲内に入る全ての変更や修正を包含するものとする。

4. 図面の簡単な説明

第1図は、本発明による基本的なコンピュータソフトウェア保安/請求システムのブロック図、そして

第2図は、本発明によってアプリケーションプログラムを適切に動作させるためにスタートプログラム及び保安プログラムがたどるステップを示したフローチャートである。

10・・・パーソナルコンピュータ

12・・・ディスク駆動装置

- 14・・・ディスク
- 16・・・保安モジュール
- 18・・・固定メモリ装置
- 20・・・請求モジュール

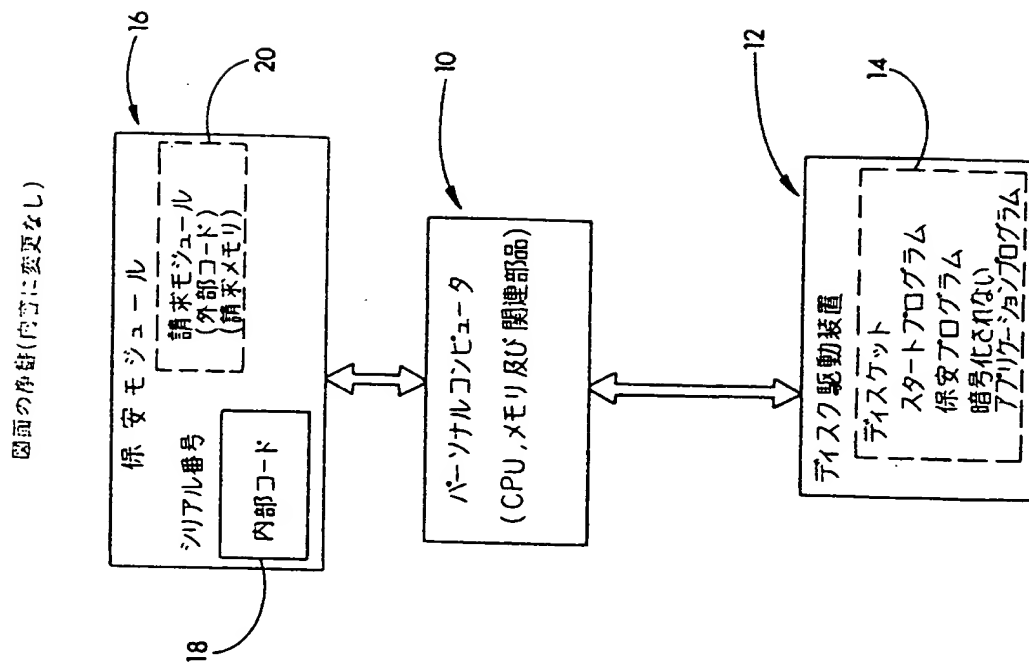


FIG. 1

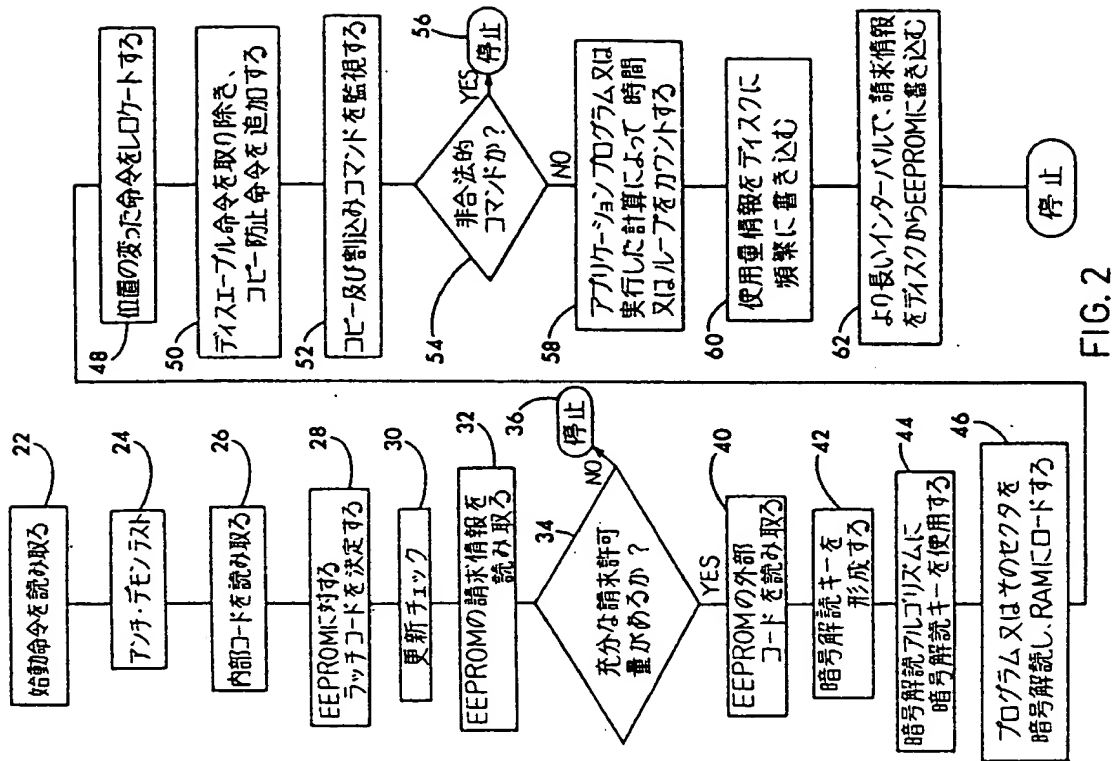


FIG. 2

手続補正書(方式)

63. 2. 18

昭和 年 月 日

特許庁長官 小川 邦夫 殿

1. 事件の表示 昭和62年特許願第268022号

2. 発明の名称 コンピュータソフトウェア用の請求システム

3. 補正をする者
事件との関係 出願人

氏名 ジョン ディヴィッド ヴィードマー

4. 代理人

住所 東京都千代田区丸の内3丁目3番1号
電話(代) 211-8741

氏名(5995) 弁理士 中村 社

5. 補正命令の日付 昭和63年1月26日

6. 補正の対象 全図面

7. 補正の内容 別紙の通り

願書に最初に添付した図面の浄書
(内容に変更なし)

万
事
立

